UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	Case No. CR19-159RSL ORDER DENYING MOTION TO DISMISS COUNTS 2 THROUGH 8

This matter comes before the Court on defendant Paige Thompson's "Motion to Dismiss Counts 2 through 8 of the Second Superseding Indictment" (Dkt. # 123).[1] Defendant faces an upcoming trial for charges of wire fraud, violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), access device fraud, and aggravated identity theft. Dkt. # 166. She contends that Counts 2 through 8 of the indictment, which allege violations of the Computer Fraud and Abuse Act (CFAA), must be dismissed for failure to state a claim. Dkt. # 123 at 1. Defendant also moves to dismiss these counts because, as alleged, they violate her Fifth Amendment right to due process and First Amendment right to free speech and expression. *Id.*

[1] The government introduced a Second Superseding Indictment (Dkt. # 166) after briefing for this motion was submitted. Because the Second Superseding Indictment does not substantively modify Counts 2 through 8, the Court reads the arguments in the present motion as applying equally to both versions of the Superseding Indictment and applies this ruling to the Second Superseding Indictment.

I. Motions to File Overlength Response and Reply

As a threshold matter, the Court grants the government's motion to file an overlength response (Dkt. # 134). The government may file a thirteen-page response. The Court also grants defendant's motion to file an overlength reply (Dkt # 159). Defendant may file a ten-page reply.

II. Counts 2 Through 8: Failure to State a Claim

Defendant argues that Counts 2 through 8 of the Indictment must be dismissed because they fail to allege criminal activity. Dkt. # 123 at 1; Fed. R. Crim. P. 12(b)(3)(B)(v). At this motion to dismiss stage, "the issue in judging the sufficiency of the indictment is whether the indictment adequately alleges the elements of the offense and fairly informs the defendant of the charge, not whether the Government can prove its case." *United States v. Buckley*, 689 F.2d 893, 897 (9th Cir. 1982). On a motion under Federal Rule of Criminal Procedure 12, the failure to allege facts that, if proven, would satisfy an essential element of the offense is a fatal defect requiring dismissal of the indictment. *See United States v. Omer*, 395 F.3d 1087, 1089 (9th Cir. 2005). However, "[t]he Government need not allege its theory of the case or supporting evidence, but only the 'essential facts necessary to apprise a defendant of the crime charged.'" *Id.* (quoting *United States v. Markee*, 425 F.2d 1043, 1047-48 (9th Cir. 1970)). An indictment need not explain all factual evidence to be proved at trial. *United States v. Blinder*, 10 F.3d 1468, 1476 (9th Cir. 1993).

In evaluating a motion to dismiss, the Court accepts the allegations in the indictment as true and is "bound by the four corners of the indictment." *United States v. Boren*, 278 F.3d 911, 914 (9th Cir. 2002). The indictment must be "construed according to common sense, and interpreted to include facts which are necessarily implied." *United States v. Berger*, 473 F.3d 1080, 1103 (9th Cir. 2007) (internal quotation marks and citation omitted). A Rule 12(b)(3)(B) motion is "capable of determination before trial if it involves questions of law rather than fact" and therefore does not intrude upon "the province of the ultimate finder of fact." *United States v. Kelly*, 874 F.3d 1037, 1046-47 (9th Cir. 2017) (quotations omitted).

Here, Counts 2 through 7 charge defendant with violating § 1030(a)(2) of the CFAA. This section prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" and "thereby obtain[ing] . . . information contained in a financial record of a financial institution" or "information from any protected computer." 18 U.S.C. § 1030(a)(2)(A), (C). Count 8 charges defendant with violating § 1030(a)(5)(A), which prohibits causing "the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). Both statutory sections include the element that defendant acted "without authorization."

The indictment alleges that defendant created proxy scanners that allowed her to identify Amazon Web Services (AWS) servers with misconfigured web application firewalls that permitted outside commands to reach and be executed by the servers. Dkt # 166 at ¶ 12. Defendant then sent commands to the misconfigured servers to obtain security credentials for particular accounts or roles belonging to the victims. *Id.* at ¶¶ 11-13, 16-18. Defendant then used these "stolen credentials" to "copy data, from folders or buckets of data" in the victims' cloud storage space and set up cryptocurrency mining operations on the victims' rented servers. *Id.* at ¶¶ 14-15, 21. The indictment further alleges that defendant concealed her location and identity while executing these actions by using VPNs and TOR.[2] *Id.* at ¶¶ 17-18.

Defendant contends that the indictment fails to allege an offense because the government, under the facts alleged, cannot prove that defendant accessed a computer "without authorization.".[3] Dkt. # 123 at 1. In particular, defendant argues that because the victim servers

[2] VPNs (virtual private networks) and TOR (The Onion Router) are both technologies that facilitate online privacy and can be used to conceal a user's identity and/or location.

[3] Counts 2 through 7 are charged under CFAA subsection (a)(2), which requires "intentionally *access[ing] a computer* without authorization." 18 U.S.C. § 1030(a)(2). In contrast, Count 8 is charged under CFAA subsection (a)(5)(A), which requires "intentionally *caus[ing] damage* without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). The Court is cognizant of the need for congruence among these subsections. *See Nosal II*, 844 F.3d at 1033. However, to the extent that defendant's arguments are focused on whether she allegedly *accessed a computer* without authorization,

were misconfigured in such a way that they automatically provided her with credentials in response to certain legitimate commands that she sent, she had received "authorization." Dkt. # 123 at 6. The government, relying on tenets of trespass law,[4] argues the computer system disclosed the credentials by "mistake, not authorization," given defendant misrepresented herself as an authorized user. Dkt. # 135 at 6 (citing to Restatement (Second) of Torts §§ 173-74 (Am. L. Inst. 1977) (explaining that consent is not a valid defense to trespass when consent is obtained by fraud, misrepresentation, or mistake)).

"Without authorization" is not defined in the CFAA. The Ninth Circuit has explained that "'without authorization' is an unambiguous, non-technical term [to be] given its plain and ordinary meaning," *United States v. Nosal (Nosal II)*, 844 F.3d 1024, 1028 (9th Cir. 2016), and has held that "a person is 'without authorization' under the CFAA 'when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission).'" *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009)). In its only opinion interpreting the CFAA, the Supreme Court explained that the "without authorization" clause "protects computers themselves by targeting so-called outside hackers – those who 'access a computer without any permission at all.'" *Van Buren v. United States*, 141 S. Ct. 1648 (2021) (quoting *Brekka*, 581 F.3d at 1133). The Supreme Court explained that liability "stems from a gates-up-or-down inquiry – one either can or cannot access a computer system." *Id.*

the Court notes that these arguments are not applicable to Count 8, which requires different elements than Counts 2-7.

[4] Notably, the Supreme Court's *Van Buren* decision counseled against reliance on common law principles when interpreting the CFAA. *See* 141 S. Ct. at 1655 n.4 (explaining that "common-law principles 'should be imported into statutory text only when Congress employs a common-law term'— not when Congress has outlined an offense 'analogous to a common-law crime without using common-law terms'" (quoting *Carter v. United States*, 530 U.S. 225, 265 (2000)). In this case, the Court need not resort to trespass law to parse an answer – prior cases interpreting the CFAA provide support for upholding the indictment.

Under this standard, the indictment here adequately states an offense. To reach this conclusion, the Court addresses each of defendant's three main arguments: (1) that authorization was granted to her by the misconfigured servers; (2) that she did not use another person's password; and (3) that she merely accessed publicly available information.

1. Authorization

Turning first to how defendant gained the credentials she used to allegedly copy the data and pursue her cryptomining operation, defendant repeatedly argues that she could not have been an "unauthorized" user because authorization was "automatically granted" to her when the misconfigured servers provided her with the user credentials. Dkt. # 160 at 9. Ultimately, defendant argues, even if authorization was a "mistake," it was "authorization nonetheless." *Id.*

Defendant cites to no case where a user's "authorization" was granted by mistake or by a purely technological process. This argument is undermined by Ninth Circuit precedent, which makes clear that "authorization" is something that only the owner of the computer or similar authority can provide. *See Nosal II*, 844 F.3d at 1028 (explaining that "'without authorization' . . . means accessing a protected computer without permission"); *Brekka*, 581 F.3d at 1133 (defining "authorization" as "permission or power granted by an authority"); *Domain Name Comm'n Ltd. v. DomainTools LLC*, 449 F. Supp. 3d 1024, 1027 (W.D. Wash. 2010) (finding "one is authorized to access a computer when the owner of the computer gives permission to use it"). Here, the indictment clearly alleges that the security credentials were "stolen" and that defendant "lacked authority to use the accounts and roles and send the commands." Dkt. # 166 at ¶ 16. The allegation that they were stolen implies that defendant acted without permission from the owner of the computer, and, therefore, without authorization.

Furthermore, prior cases make clear that there is a difference between the technical ability to access a computer and "authorization" to access a computer. For example, in *Brekka* the Ninth Circuit explained that where a former employee's login credentials had not been deactivated after he left the company, there was "no dispute that if [the employee had] accessed [his former employer's] information on the [traffic monitoring] website after he left the company . . . , [the employee] would have accessed a protected computer 'without authorization' for purposes of the CFAA." 581 F.3d at 1136. Indeed, an order from this Court, cited frequently by defendant, found that where the plaintiff computer owner had explicitly revoked defendant's permission to access its servers, any subsequent access by defendants was "without authorization" even though, technologically speaking, defendant still had the *ability* to access the servers. *DomainTools*, 449 F. Supp. 3d at 1027-28; *see also Facebook, Inc.*, 844 F.3d at 1067 ("Once permission [from the computer owner] has been revoked, technological gamesmanship . . . will not excuse liability"). Thus, merely having the technological capability to access a computer is not synonymous with "authorization."

These conclusions, of course, go only to the sufficiency of the indictment. *See Buckley*, 689 F.2d at 897. Any argument that mistake or technological process rendered defendant "authorized" is properly resolved by the trier of fact.

2. Passwords

Defendant argues that once inside the servers, she "did not use another person's password or send 'brute force' commands to gain any further access." Dkt. # 160 at 9. Instead, the system "granted her access" in response to a set of commands because it mistook her for an "authorized visitor." *Id.* Defendant's argument is essentially that because she is alleged to have found a key rather than smashed the window, she cannot have been "without authorization."

Determining authorization under the CFAA requires a "gates up or down" inquiry. *Van Buren*, 141 S. Ct. at 1658. Courts have long held that technologically bypassing an authentication requirement is unauthorized access under the CFAA. *See United States v. Morris*, 928 F.2d 504, 506 (2d Cir. 1991) (describing computer program that guessed passwords or found other unintentional holes to gain access); *United States v. Phillips*, 477 F.3d 215, 219-21 (5th Cir. 2007) (describing computer program that scanned computer network for vulnerabilities and used those vulnerabilities to gain access); *see also* Orin Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1171-73; *cf. Van Buren*, 141 S. Ct. at 1654 (finding that defendant "access[ed] a computer with authorization" when he used his patrol-car computer and valid credentials to log into the law enforcement database").

Here, regardless of the technological process defendant used to obtain the security credentials, the indictment clearly states that she accessed the data by using "stolen credentials" belonging to "accounts and roles of those customers that had permission to view and copy data." Dkt. # 166 at ¶ 11. Thus, the indictment adequately alleges that the gates were "up" for defendant, as she was not herself an authorized user. *See Nosal II*, 844 F.3d at 1038 (finding defendant acted "without authorization" where he logged into his former employer's computer system with another individual's credentials after his own credentials were affirmatively revoked). To the extent defendant wishes to argue that her access method was authorized, such arguments should be raised to the trier of fact.

3. Public Information

Defendant's most compelling argument is that because the victims' firewalls were misconfigured, "anyone with a proxy scanner" could have identified and entered the victim servers, and thus defendant should be "no more liable under the CFAA than a person accessing a public-facing web page." Dkt # 123 at 6.

Courts have declined to find a CFAA violation where the information accessed by the defendant is public facing. *See, e.g.*, *Cvent v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 933-34 (E.D. Va. 2011) (holding competitor's use of a scraper to query a company's website was authorized access under the CFAA because "the entire world was given unimpeded access to [the] website"); *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 303-04 (6th Cir. 2011) (finding labor union's use of builder's telephone and e-mail systems was authorized because defendants "only targeted computer systems that [the builder] made available to the public"). However, this has not been true across the board. *See United States v. Auernheimer*, No. CR11–470SDW, 2012 WL 5389142, at *2 (D.N.J. Oct. 26, 2012), *rev'd on other grounds*, 748 F.3d 525 (3d Cir. 2014) (convicting defendant of unauthorized access for using a software program that collected information from an AT&T website at hard-to-guess, but public facing, URL addresses intended to be customer specific). Indeed, a recent opinion by the Ninth Circuit, which concluded that it was "likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA," was vacated and remanded by the Supreme Court for further consideration in light of *Van Buren*. *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003 (9th Cir. 2019), *cert. granted, judgment vacated*, 141 S. Ct. 2752 (2021) (mem.).

While the *Van Buren* opinion declined to define exactly when a "gate" is "up" or "down," the Supreme Court hinted that it was more likely to find "gates up" where there was some authentication requirement. *Van Buren*, 141 S. Ct. at 1658-59 & nn.8-9. The question of whether accessing a server that is not meant to be public (unlike a public facing website) but nonetheless lacks protective authentication requirements constitutes acting "without authorization" under the CFAA therefore exists in a gray area.[5] However, the Court need not resolve this question here.

Here, defendant may be able to argue that, prior to using the allegedly stolen security credentials, she was merely viewing "information for which access is open to the general public and permission is not required." *LinkedIn*, 938 F.3d at 1001-02. However, this argument is properly made to the trier of fact. Further, even if this argument has merit, it only affects *where* in the chain of events the CFAA offense might attach, rather than *whether* one attaches at all. While using a proxy scanner to identify and initially access misconfigured servers may not qualify as a CFAA violation under the "gates up" formulation expounded in *Van Buren*, the allegations that defendant obtained and used security credentials that did not belong to her, and that she was not authorized by the victims to use, adequately state an offense under the CFAA.

For all of the foregoing reasons, defendant's motion to dismiss Counts 2 through 8 for failure to state a legally cognizable CFAA claim is denied.

[5] Recognized CFAA commentator Professor Orin Kerr has explained that *Van Buren* "leaves to lower courts the largely interstitial work of figuring out the hard line-drawing of what exactly counts as enough of a closed gate to trigger liability." Orin Kerr, *Focusing the CFAA in* Van Buren, SUP. CT. REV. (forthcoming).

III. Due Process

Defendant further argues that Counts 2 through 8 of the indictment should be dismissed as unconstitutionally vague because they violate her Fifth Amendment right to due process. Dkt. # 123 at 8.

In the Ninth Circuit, "[t]o survive vagueness review, a statute must (1) define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited; and (2) establish standards to permit police to enforce the law in a non-arbitrary, non-discriminatory manner." *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007) (internal quotations and citation omitted). Here, defendant argues that the CFAA charges in the indictment fail on both counts. First, she argues, "[n]othing in the text of the CFAA, or the legal opinions that have interpreted it since its passage" would put defendant on notice that her conduct would subject her to criminal liability. Dkt. # 123 at 10. Second, she argues that the government's use of the CFAA to prosecute her for behavior akin to that of a "white hat hacker" is unconstitutionally arbitrary. *Id.*

1. Fair Notice

Defendant's claim that the CFAA does not provide her with fair notice of the criminal nature of her conduct is unconvincing. To begin, defendant consistently characterizes her conduct as using "a proxy scanner to detect 'open gates' on servers connected to the Internet." *Id.* However, the indictment charges defendant with far more than this. As discussed above, the indictment charges defendant with not only using a proxy scanner to detect "open gates," but then sending commands through those open gates to steal security credentials, and finally using those stolen credentials to copy data and set up cryptomining operations. Dkt. # 166 at ¶¶ 12-21. As addressed in the previous section, the allegations in the indictment reasonably state a claim for a violation of the CFAA in light of the statute's text and judicial opinions interpreting the statute. *Cf. United States v. Lanier*, 520 U.S. 259, 266 (1997) ("[D]ue process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope.").[6]

To the extent that defendant analogizes herself to "white hat hackers," there has long been concern among the security researcher community about how their actions may be criminal under the CFAA. *See, e.g.*, Brief of Amicus Curiae Computer Security Researchers, *Van Buren*, 141 S. Ct. 1648 (No. 19-783), 2020 WL 4005654.

Considering these factors, the Court finds defendant had fair notice of the potential criminal liability of her actions.

2. Arbitrary Enforcement

Defendant's claim that the CFAA charges against her amount to arbitrary enforcement is also unavailing. First, defendant argues that her conduct was "almost identical" to that of a "white hat hacker." Defendant cites to a number of media articles to support the contention that numerous federal agencies and companies actively engage and reward white hat hackers. Dkt. # 160 at 2 n.1. However, far from proving her point that *she* is a white hat hacker, the articles appear to undermine her claim. In one article, the hacker returned the heisted digital coins and explained that they had carried out the attack "for fun" and to expose a vulnerability. The article was also keen to note that the hacker is "still unidentified," which would make prosecution difficult. *See* Miranda Bryant, *'White Hat' Hacker Behind $610m Crypto Heist Returns Most of*

[6] To the extent that defendant invokes the rule of lenity in her due process argument, that defendant was aware her behavior was criminal weighs heavily against its application. *See, e.g.*, *United States v. Nader*, 542 F.3d 713, 721 (9th Cir. 2008) (counseling against application of the rule of lenity where defendants "knew that their conduct was illegal" because "the rule of lenity . . . 'is rooted in fundamental principles of due process which mandate that no individual be forced to speculate, at peril of indictment, whether his conduct is prohibited'" (quoting *Dunn v. United States*, 442 U.S. 100, 112 (1979)). As the government points out, there is compelling evidence that defendant herself was personally aware of the potential criminal and legal ramifications of her conduct. Not only was she an experienced systems engineer, but the government has also marshaled evidence showing that defendant was aware of the prosecution of Adrian Lamo, a gray hat hacker "who was arrested, indicted, and convicted for accessing the New York Times' intranet without authorization – through a misconfigured proxy server – in violation of the CFAA." Dkt. # 135 at 11. In fact, defendant described her own activities as "way worse than what [Lamo] got arrested for initially." *Id.* It follows, then, that defendant was aware of the risk she was taking and the potential criminal liability that could attach to her conduct.

Money, The Guardian (Aug. 13, 2021), https://www.theguardian.com/technology/2021/aug/13/white-hat-hacker-behind-610m-crypto-heist-returns-most-of-money. In another, the article reports that white hat hackers "report[ed]" a vulnerability in an Ethereum network's "proof-of-stake Genesis contract," allowing it to resolve the bug. The article also separately refers to a "malicious hacker" who stole digital tokens before the bug was resolved. The article fails to provide sufficient detail to compare defendant's conduct with that of the various hackers mentioned in the article and describes a highly different context than the one the Court is confronted with here. However, given that defendant is alleged to have copied vast quantities of data to her own machine, her behavior appears more closely analogous to that of the so-called "malicious hacker" than that of the "white hat hackers." *See* Brian Quarmby, *Polygon Upgrade Quietly Fixes Bug That Put $24B of MATIC at Risk*, CoinTelegraph (Dec. 30, 2021), https://cointelegraph.com/news/polygon-upgrade-quietly-fixes-bug-that-put-24b-of-matic-at-risk. Finally, the Department of Homeland Security program defendant touts is clear that it includes only "*vetted* cybersecurity researchers who *have been invited* to access select external DHS systems." Press Release, Dep't of Homeland Sec., DHS Announces "Hack DHS" Bug Bounty Program to Identify Potential Cybersecurity Vulnerabilities (Dec. 14, 2021), https://www.dhs.gov/news/2021/12/14/dhs-announces-hack-dhs-bug-bounty-program-identify-potential-cybersecurity. In contrast, defendant was neither vetted nor invited to access AWS or individual victims' servers. This factual difference has significant ramifications under the CFAA, where, as discussed above, the question is whether the user has "authorization" from the computer owner.

Defendant also argues that apart from the security researcher argument, she is just one of many individuals who "scan the internet, communicate with publicly facing websites, obtain information from the websites, and save the information on their computers." Dkt. # 123 at 11. Again, defendant mischaracterizes the allegations laid out against her in the indictment – most critically to the CFAA counts, that she employed user credentials she was not authorized to use. Her related argument that had she "acted less erratically (rather than a person who has struggled her entire life with mental illness and her gender identity) and notified Capital One through its

Responsible Disclosure Program (rather than alerting the information security community at large of the events in question), she surely would not have been charged," Dkt. # 160 at 1, is based on a counterfactual hypothetical, which the Court need not address.[7] Accordingly, the indictment adequately alleges a CFAA violation and defendant has not shown that this prosecution is being pursued in an arbitrary or discriminatory manner.

Because defendant had adequate notice of potential criminal liability, and cannot show arbitrary enforcement, her motion to dismiss for violation of due process rights is denied.

IV. First Amendment

Finally, defendant argues that Counts 2 through 8 of the indictment violate her First Amendment rights, and thus must be dismissed. Dkt # 123 at 11-13. An as-applied First Amendment challenge "contends that the law is unconstitutional as applied to the litigant's particular speech activity." *United States v. Kaczynski*, 551 F.3d 1120, 1126 (9th Cir. 2009) (quoting *Foti v. City of Menlo Park*, 146 F.3d 629, 635 (9th Cir. 1998)). Here, the speech activity claimed by defendant includes (1) scripting code; and (2) receiving information that the owner of a computer makes publicly available. Dkt # 123 at 12.[8]

Assuming that the code defendant scripted in creating the proxy scanner would be protected by the First Amendment, *see, e.g.*, *United States v. Bondarenko*, No. CR17-306, 2019 WL 2450923, at *10 (D. Nev. June 12, 2019), it is hard to see how the CFAA prosecution here impedes the exercise of this protected speech. Neither creating nor using the proxy scanner is alone alleged to constitute accessing a computer "without authorization" in violation of the CFAA. To the extent that defendant claims code she allegedly wrote to obtain and facilitate using the "stolen" security credentials is protected speech, the Supreme Court has explained that

[7] While this is not a decisive point for deciding this Motion to Dismiss, it would be an important factor at sentencing.

[8] To the extent that defendant claims that the government is criminalizing her exercise of free speech inherent in her choice "to notify the community at large that Capital One was inappropriately storing its customers' personal information in areas of AWS servers accessible to even the most novice hacker," rather than "privately notify[ing] Capital One of its error," Dkt. # 160 at 5-6, the indictment is silent as to who she did and did not notify. This too would have more relevance at sentencing.

the First Amendment does not protect "speech integral to criminal conduct." *United States v. Stevens*, 559 U.S. 460, 468 (2010). Because the code defendant wrote to access the victims' data and set up her cryptomining operations was "integral" to her alleged criminal conduct, it is not protected speech.

Defendant also argues that receiving information "the owner of a computer makes publicly available" qualifies as protected speech.[9] Dkt. # 123 at 2. Assuming, *arguendo*, that this is true, defendant's argument that her right to engage in this protected speech is violated by the indictment can only stand if the information on the victims' servers was, in fact, publicly available. As discussed above, the Court finds that the government has adequately alleged that when defendant used security credentials belonging to another to access data stored on the victims' servers, she was not accessing "publicly available information" but was instead accessing a computer without authorization.[10] Thus, defendant's alleged conduct, as described in the indictment, does not include receiving "publicly available" information and thus would not implicate her First Amendment rights in that protected activity. While defendant is free to dispute the facts alleged in the government's indictment at trial and may argue that contrary to the government's characterization, the data *was* publicly accessible, such a defense is not ripe for pretrial determination. *United States v. Covington*, 395 U.S. 57, 61 (1969) (explaining that a defense is capable of pretrial determination "if trial of the facts surrounding the commission of the alleged offense would be of no assistance in determining the validity of the defense").

[9] While it's undisputed that the First Amendment protects a right to "receive information and ideas," *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748, 757 (1976), the case defendant cites to support the proposition that the First Amendment protects "white hat hacking, data mining, scraping, and access to publicly available resources on the Internet," Dkt. # 123 at 12, dealt with a content- and speaker-based restriction on the sale, disclosure, and use of prescriber-identifying information in pharmacy records, not with publicly available information. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 563-64 (2011).

[10] To the extent defendant seeks to argue that *some* of the behavior described in the indictment does not constitute a crime under the CFAA (and that charging this conduct as such would be a violation of First Amendment rights), such a determination is better resolved in the context of determining the point at which defendant accessed a computer "without authorization." *See* Section II.3.

Defendant agrees that the CFAA prohibits “breaking and entering” protected computers but argues that the government’s application of the statute to her conduct “runs afoul of the First Amendment” because her conduct does not qualify as “breaking and entering” under the CFAA.[11] Dkt. # 160 at 5. However, as discussed, the indictment adequately alleges that defendant accessed a computer without authorization. The indictment therefore limits application of the CFAA to the “breaking and entering” of protected computers and does not violate defendant’s First Amendment rights. Accordingly, defendant’s motion to dismiss for violation of her First Amendment rights is denied.

V. Conclusion

For all of the foregoing reasons, IT IS HEREBY ORDERED that:

1. Defendant’s motion to dismiss Counts 2 through 8 of the indictment (Dkt. # 123) is DENIED.
2. The government’s motion to file an overlength response (Dkt. # 134) is GRANTED.
3. Defendant’s motion to file an overlength reply (Dkt # 159) is GRANTED.

DATED this 21st day of March, 2022.

Robert S. Lasnik
United States District Judge

[11] Defendant cites to *Sandvig v. Barr*, 451 F. Supp. 3d 73, 88-89 (D.D.C. 2020) and *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) to argue that the government “has attempted to criminalize speech utilizing the CFAA.” Dkt. # 160 at 4-5. However, both *Sandvig* and *Drew* dealt with violations of a website’s Terms of Service agreement pre-*Van Buren*. The potential for contract-based limits on “authorization” under the CFAA has been the primary source of concern for potential First Amendment violations. *See* Orin Kerr, *Cybercrime's Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1658-59 (2003). In contrast, defendant is charged with technological circumvention of authentication.